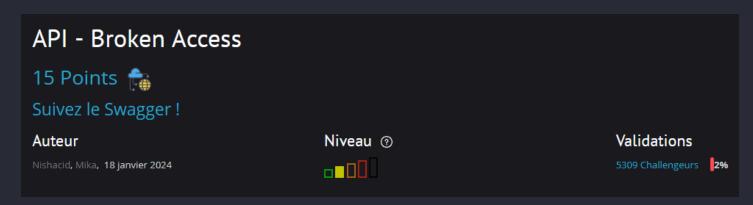
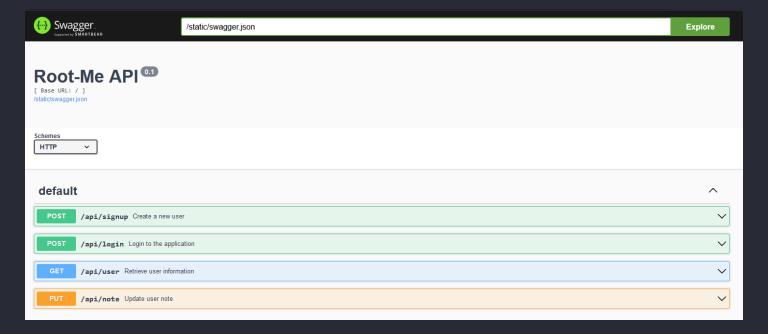
API Broken Acess



Énoncé

Votre ami a mis en place une plateforme où vous pouvez vous inscrire et mettre une note privée. Tout est fait sur la base d'une API. Avant de mettre en place le Front-End, il vous a demandé de vérifier que tout était sécurisé.

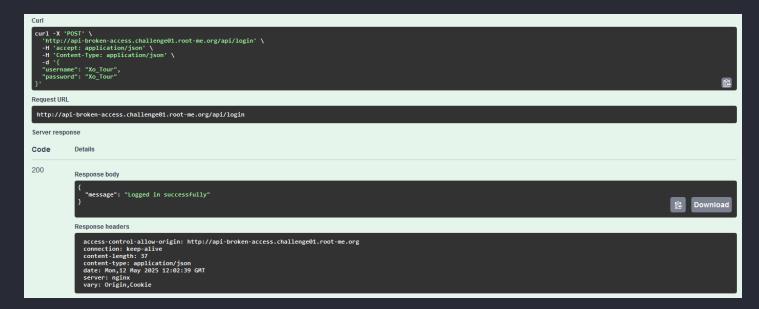
Web Site



new user

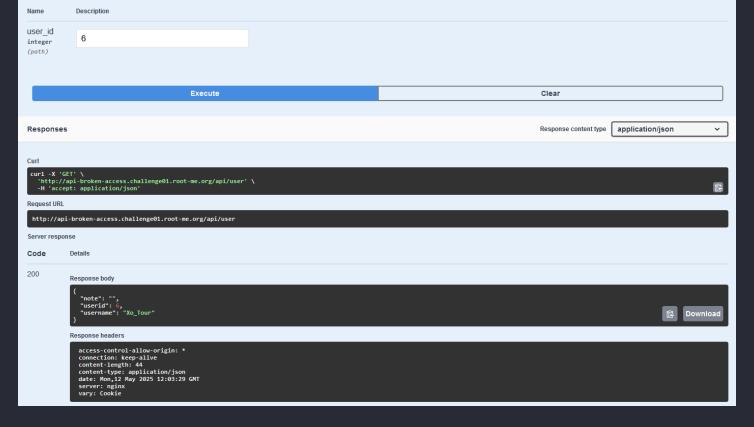
```
Curl "PoSt" \ "http://api-broken-access.challenge01.root-me.org/api/signup' \ -H "content-iype: application/json' \ -H "content-iype: application/json' \ -I "content-iype: application/json content-iype: application/j
```

login



user info(s)

Par défaut, l'ID affiché sera l'utilisateur loggé, avec n'importe quel ID tapé :



user note



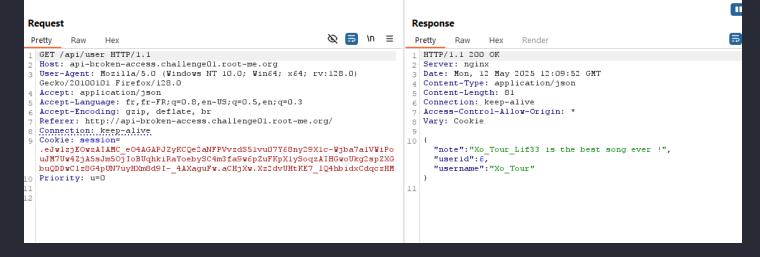
Toutes les options testés, maintenant il faut trouver le Broken Access.

Broken Access

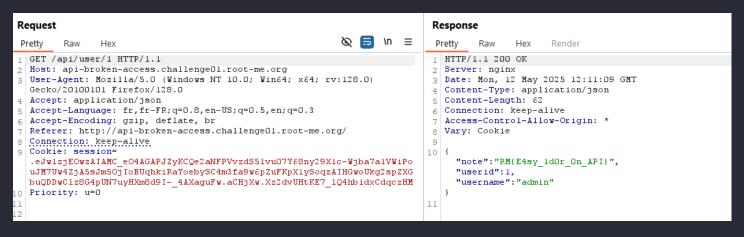
L'option qui a retenue mon attention, est le 'user information' :

burp

Si j'intercepte la requête avec BURP:



Maintenant, est-ce que je peux changer l'URL en ajoutant /1 réservé aux ID admin/root :



"note":"RM{E4sy_1d0r_0n_API}","userid":1,"username":"admin"